WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Teresa Lunt, PM DARPA/ITO, Sponsor**
- **Howie Shrobe, PM, DARPA/ITO**
- **Hilarie Orman, PM, DARPA/ITO**
- **Karl Levitt, UC Davis, Chair**

Report Summary

- **Problem Description / Technical Scope**
  - **Survivable systems: How to**
    - **design**
    - **build**
    - **validate**
    - **deploy**

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Relevant Disciplines:**
- **fault tolerance**
- network management
- multi-agent planning
- safety engineering
- software engineering
- economics
- testing, specification
- statistical analysis
-

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Relevant Disciplines**
- risk management
- alarm correlation
- distributed system design
- immunology
- security
- control systems

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Relevant Technologies**
- statistical anomaly detection
- autodiscovery, alarm correlation
- space-time adaptive processing to pick targets out of clutters
- configuration states
- network management
- hot swappable recovery techniques

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Major Technical Challenges**
- Guaranteeing some level of service during attack
- Collaboration between detection/response
- Coordination among distributed survivable agents
- technologies for quantifiable, predictable survivability, e.g. replication
- Understanding and quantifying recovery, different paradigms for recover, what are the issues
- taxonomy of failures and recovery
- immunized recovery

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Major Technical Challenges**
- new vulnerablities from mobile systems
- survivability issues in new technology
- adaptive response to faults of different types
- fail fast
- unknown attacks
- Complexity
- Distributed, coordinated attacks

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Major Technical Challenges**
- Theoretical basis for faults other than h/w faults
- Probablistic guarantee of service without having a hard core
- Acceptance of survivability solutions
- Cooperation across domains
- Denial of service

Addressing the Challenges

- Approach
  - Design Methodology
  - Knowledge Acquisition/ Presentation
  - Systems Concepts
  - Performance Eval/Validation
  - Application Testbeds

Design Methodologies for Survivability Technology

- Proactive detection and distribution
  - Continuously learn from antigens and pass through the network
- Combine multiple technologies
  - multiple defenses
- Adaptability for rapid recovery
  - Self-repairing functions
- Guaranteeable network characteristics
  - reasonable environment for survivability

WG#16: Surviving Intrusions in Large-Scale Systems

Design Methodologies for Survivability Technology

- Response to attacks and attackers
  - eradicate the antigen
- Extend network management, QoS metrics
  - meet the survival goal of the species
  - competing species
- Defenses against insiders
  - auto-immune disease
- Peaceful coexistence with other networks
  - move the tribe

WG#16: Surviving Intrusions in Large-Scale Systems

Knowledge Acquisition and Presentation

- What to measure, what to learn
  - at what resolution
  - where in the network layer
- Modeling of network architecture, services
  - to understand normalcy
- Predictive attack generation
- Continuous learning of profiles
- Visualization, HCI

Systems Concepts

- Adaptable network components for rapic and remote “swap in” capability:
  - sensors
  - analysis systems
  - response systems

Performance and Validation

- What, how, where, to measure network state
- Red teams and stress tests
- Quantification of losses, rapidity of change, number of successful prosecutions

Application Testbeds

- Power grid
  - new, emergent industry changes
- Financial
  - years of experience
  - global reach
- Phone
- Industry incentives to deploy

Outcomes

- Design methodology
- Specific services that should be added in for survivability (analogous to authentication for secure systems) for various levels of survivability
- Survivability metrics
- Validation methodology
- New automated recovery techniques
- Operational worldwide networks
- Experiments on DARPA's testbeds

Outcome (cont)

- Immunization mechanisms, immune system response
  - Generalize from what you know, when you see you've been damaged, then customize a defense
  - Genetic algorithms to generate new attacks from old ones
  - Beware of auto-immune disease
- Circuit breakers
- Attack libraries development
- Exchange of profiles, hot lists

Outcome (cont)

- Attack libraries development
- Exchange of profiles, hot lists
- Exchange of info on detected attacks: some signature, problem profile or indicators, or even vaccination (careful not to cause more harm)
- need facility for proof of safety and efficacy of vaccines: FDA
- Better personal hygiene

Likelihood of Success

- Expect the unexpected
- We’re never done; new technologies introducte new vulnerabilities, and we keep discovering new vulnerabilities in old technologies

Programmatics

- Scale of effort: BIG
  - National security problems, global, financial
- Why DARPA? Long-term high-risk research, others aren't doing it, and DoD has the problem. Provides leverage to various industries to facilitate transition to commercialization or commercial use
- Other collaborators: CIA, NSA, power, FAA, FBI, telcos, financial community, commerce
- What if we don't do this: we will be at risk with or will not be able to take advantage of new technologies. E.g. e-commerce

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Problem Description / Technical Scope**
  - **detection of large-scale coordinated attacks**
  - **domino effects, side effects**
  - **predict choke points where an enemy would attack**
  - **what will be attacked: network or apps?**

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Problem Description / Technical Scope**
  - **detection across global networks**
  - **being able to detect what kind of attack is going on**
  - **latent attacks, that could perhaps coordinate themselves**
  - **how to do anomaly detection in a crisis**

WG#16: Surviving Intrusions in Large-Scale Systems

Report Summary

- **Problem Description / Technical Scope**
  - **correlation**
  - **how to reserve enough bandwidth for critical apps**
  - **multilevel availability**
  - **design in dependability to infrastructure systems**
  - **bound losses**

Projected Outcome

- Outcome 1
  - details / examples / justification
  - expected likelihood of success
- Outcome 2
  - details / examples / justification
  - expected likelihood of success
- ...

Investment Strategy

- DARPA, Industry Support
  - Why DARPA?
    - DoD impact
    - Infrastructure protetion
  - What other collaborations?
    - NSA, CIA, FBI, FAA, AFIWC
    - Financial community
    - Telcos, power utilities
- What if we did not do this?

Other Issues Addressed

- What if we did not do this?
  - Nat'l vulnerabilities
  - No new emerging technology
- Optimal Scale of Efforts
  - small vs large? mix?
    - significant growth potential